#2

Docket No.: 57454-054 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	
	:	
Tsukawa OOISHI	:	
	:	
Serial No.:	:	Group Art Unit:
	:	
Filed: April 3, 2001	:	Examiner:

For: AUTHENTICATION APPARATUS FOR AUTHENTICATION TO PERMIT ELECTRONIC DOCUMENT OR PAYMENT BY CARD USING PERSONAL INFORMATION OF INDIVIDUAL, VERIFICATION APPARATUS FOR VERIFYING INDIVIDUAL AT PAYMENT SITE, AND ELECTRONIC AUTHENTICATION SYSTEM INTERCONNECTING THE SAME

CLAIM OF PRIORITY AND TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Commissioner for Patents
Washington, DC 20231

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicant hereby claims the priority of:

Japanese Patent Application No. 2000-355565,
Filed November 22, 2000

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Stephen A. Becker
Registration No. 26,527

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 SAB:ykg
Date: April 3, 2001
Facsimile: (202) 756-8087

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年１１月２２日

出 願 番 号
Application Number: 特願２０００－３５５５６５

出 願 人
Applicant (s): 三菱電機株式会社

２００１年 ２月 ９日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２００１－３００５１３８

【書類名】　特許願
【整理番号】　526800JP01
【提出日】　平成12年11月22日
【あて先】　特許庁長官殿
【国際特許分類】　G06K 17/00
G06K 19/10
G06F 19/00
【発明者】
【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
【氏名】　大石　司
【特許出願人】
【識別番号】　000006013
【氏名又は名称】　三菱電機株式会社
【代理人】
【識別番号】　100064746
【弁理士】
【氏名又は名称】　深見　久郎
【選任した代理人】
【識別番号】　100085132
【弁理士】
【氏名又は名称】　森田　俊雄
【選任した代理人】
【識別番号】　100091409
【弁理士】
【氏名又は名称】　伊藤　英彦
【選任した代理人】
【識別番号】　100096781
【弁理士】

【氏名又は名称】　堀井　豊

【選任した代理人】

【識別番号】　100096792

【弁理士】

【氏名又は名称】　森下　八郎

【手数料の表示】

【予納台帳番号】　008693

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証装置、照合装置およびそれらを接続した電子認証システム

【特許請求の範囲】

【請求項１】　配布された電子署名を付加した電子書類を回収して、前記電子書類の認証を行なう認証装置であって、

第１の情報に対して、本人の身体に関連した情報を数値化して得られた独自情報を用いて第１の演算を行なって暗号化された電子署名を生成し、該電子署名を電子書類に付加するための電子署名生成手段と、

前記電子書類に付加された電子署名を抽出し、第２の演算を行なって復号化して個人の認証を行なうための個人認証手段とを含む認証装置。

【請求項２】　前記電子署名生成手段は、前記本人の独自情報を暗号化して独自ビット情報を生成するための独自ビット情報化手段と、

前記第１の情報に対して、前記独自ビット情報化手段によって生成された独自ビット情報を用いて論理演算して暗号化するための論理演算手段と、

前記論理演算手段によって暗号化された情報を電子署名として前記電子書類に付加するための電子署名付加手段とを含む、請求項１記載の認証装置。

【請求項３】　前記個人認証手段は、前記電子書類に付加された電子署名を抽出するための抽出手段と、

前記抽出手段によって抽出された電子署名に対して、前記独自ビット情報化手段によって生成された独自ビット情報を用いて論理逆演算を行なって第２の情報を生成するための論理逆演算手段と、

前記第１の情報と、前記論理逆演算手段によって生成された第２の情報とを比較して、個人の認証を行なうための比較手段とを含む、請求項１または２記載の認証装置。

【請求項４】　カードによる支払い時に本人の確認を行なう認証装置であって、

第１の情報に対して、本人の独自情報を用いて論理演算を行なって、暗号化された認識情報を生成するための認識情報生成手段と、

前記カードに予め記録された認識情報と、前記認識情報生成手段によって生成

された認識情報とを比較して本人の確認を行なうための認証手段とを含む、認証装置。

【請求項５】　前記認識情報生成手段は、前記本人の独自情報を暗号化して独自ビット情報を生成するための独自ビット情報化手段と、

前記第１の情報に対して、前記独自ビット情報化手段によって生成された独自ビット情報を用いて論理演算を行なって、前記認識情報を生成するための論理演算手段とを含む、請求項４記載の認証装置。

【請求項６】　前記認証装置はさらに、前記カードに予め記録された認識情報に対して、前記独自ビット情報化手段によって生成された独自ビット情報を用いて論理逆演算を行なって第２の情報を生成するための論理逆演算手段と、

前記第１の情報と前記論理逆演算手段によって生成された第２の情報とを比較して、個人の認証を行なうための比較手段とを含む、請求項５記載の認証装置。

【請求項７】　前記独自情報は、本人の身体に関連した情報を数値化して得られた情報である、請求項４～６のいずれかに記載の認証装置。

【請求項８】　カードによる支払い時に手書きのサインによって本人の確認を行なう照合装置であって、

前記カードに記録された認識情報に対して、暗号鍵を用いて論理演算を行なって第１のサイン情報を生成するための論理演算手段と、

前記論理演算手段によって生成された第１のサイン情報と、手書きのサインを数値化して得られた第２のサイン情報とを比較して本人であるかを検証するための一致検証手段とを含む、照合装置。

【請求項９】　前記認識情報は、第１の情報に対して、本人の独自情報を暗号化して生成された独自ビット情報を用いて論理演算を行なった情報である、請求項８記載の照合装置。

【請求項１０】　前記独自情報は、本人の身体に関連した情報を数値化して得られた情報である、請求項８または９記載の照合装置。

【請求項１１】　カードによる支払い時に手書きのサインによって本人の確認を行なう照合装置と、支払いの正当性を認証する認証装置とを接続した電子認証システムであって、

前記認証装置は、本人の独自情報を暗号化して独自ビット情報を生成するための独自ビット情報化手段と、

第１の情報に対して、前記独自ビット情報化手段によって生成された独自ビット情報を用いて論理演算を行なって、前記認識情報を生成するための第１の論理演算手段と、

手書きサインを数値化して得られた第１のサイン情報に対して、前記第１の論理演算手段によって生成された認識情報を用いて論理演算を行なって、暗号鍵を生成するための暗号キー化手段と、

前記照合装置から伝送された情報から暗証番号を抽出するための暗証番号抽出手段と、

前記暗証番号抽出手段によって抽出された暗証番号に対して、前記独自ビット情報化手段によって生成された独自ビット情報を用いて論理逆演算を行なって、第２の情報を生成するための論理逆演算手段と、

前記第１の情報と、前記論理逆演算手段によって生成された第２の情報とを比較して支払いの正当性の認証を行なうための比較手段とを含み、

前記照合装置は、前記カードに記録された認識情報に対して、前記暗号キー化手段によって生成された暗号鍵を用いて論理演算を行なって、第２のサイン情報を生成するための第２の論理演算手段と、

前記第２の論理演算手段によって生成された第２のサイン情報と、手書きのサインを数値化して得られた第３のサイン情報とを比較して本人であるかを検証するための一致検証手段とを含む、電子認証システム。

【請求項１２】　外部から支払い依頼があった時に本人の確認を行なう認証装置であって、

本人の独自情報に対して、時間とともに変化する第１の番号を用いて論理逆演算を行なって、暗号化された暗証番号を生成するための暗証番号生成手段と、

外部から受信した情報に対して、前記暗証番号生成手段によって生成された暗証番号を用いて論理演算を行ない、当該論理演算結果に基づいて本人の一致を検証する検証手段とを含む、認証装置。

【請求項１３】　前記検証手段は、本人が予め定めたサインデータに対して

、本人の独自情報を用いて論理逆演算を行なって生成されたランダム暗証を外部から受信し、前記ランダム暗証に対して、前記暗証番号生成手段によって生成された暗証番号を用いて論理演算を行なうための論理演算手段と、

外部からサインデータおよび時間とともに変化する第２の番号を受信し、前記サインデータに対して、前記第２の番号を用いて論理逆演算を行なうための番号逆演算手段と、

前記論理演算手段による論理演算結果と、前記番号逆演算手段による論理逆演算結果とを比較して、本人の一致を検証する一致検証手段とを含む、請求項１２記載の認証装置。

【請求項１４】　前記認証装置はさらに、前記独自情報に対して、前記暗証番号生成手段によって生成された暗証番号を用いて論理逆演算を行なって、時間とともに変化する第３の番号を生成するための論理逆演算手段と、

前記第２の番号と前記論理逆演算手段によって生成された第３の番号とを比較して、個人の認証を行なうための比較手段とを含む、請求項１２または１３記載の認証装置。

【請求項１５】　前記独自情報は、本人の身体に関連した情報を数値化して得られた情報である、請求項１２～１４のいずれかに記載の認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子化された書類、クレジットカード等のカードの偽造や悪用を防止するための技術に関し、特に、電子署名やカードによる支払い依頼等の認証を行なう認証装置、支払現場における本人確認のためのサイン等の照合を行なう照合装置およびそれらを接続した電子認証システムに関する。

【０００２】

【従来の技術】

従来、顧客が店頭において商品を購入する際、クレジットカード等のカードによる支払いが広く行なわれている。カードによる決済においては、カードの本人であるか否かを確認するための認証が必要であり、認証の際に手書きによるサイ

ンや暗証番号などが利用されている。

【０００３】

また、近年、インターネットの普及によって、顧客が端末を介して商品の購入等を行なう電子商取引が普及しつつある。利用者は、自身の端末を使用して商品を購入できるため、店頭に出向く必要がなくなり利便性が飛躍的に向上することとなる。

【０００４】

さらには、電子化された書類に電子署名を付加して配布し、後にその電子署名の正当性を確認することによって、書類が偽造されたものでないことを確認する技術も開発されている。

【０００５】

【発明が解決しようとする課題】

しかし、上述したカードによる決済においては、カードを紛失したり、盗難に遭ったりした場合に、暗証番号やサインが偽造されてカードが悪用されることがあった。したがって、後日本人確認によってカードの悪用が発覚したとしても、本人および支払い代行会社（クレジット会社）に対して多大な労力が発生したり、多大な損害が発生したりすることがあった。

【０００６】

また、電子商取引においては、利用者が実際にインターネットを介して商品を購入する際、利用者のクレジットカード番号や暗証番号が漏洩して悪用されることがあり、トラブルの一因となっていた。

【０００７】

さらには、電子化された書類に電子署名を付加する技術においては、電子署名の管理がまちまちであり、電子署名が容易に偽造されて悪用されたり、個人のプライバシやプロパティが不当に侵害されるという問題もあった。

【０００８】

本発明は、上記問題点を解決するためになされたものであり、第１の目的は、電子署名が偽造されて悪用されるのを防止することが可能な認証装置を提供することである。

【０００９】

第２の目的は、暗証番号やサインが偽造されてカードが悪用されるのを防止することが可能な認証装置を提供することである。

【００１０】

第３の目的は、カードによる支払い時に本人の確認を的確に行なうことが可能な照合装置を提供することである。

【００１１】

第４の目的は、インターネットを介して商品を購入する際、利用者のクレジットカード番号や暗証番号が漏洩して悪用されるのを防止することが可能な認証装置を提供することである。

【００１２】

【課題を解決するための手段】

請求項１に記載の認証装置は、配布された電子署名を付加した電子書類を回収して、電子書類の認証を行なう認証装置であって、第１の情報に対して、本人の身体に関連した情報を数値化して得られた独自情報を用いて第１の演算を行なって暗号化された電子署名を生成し、電子署名を電子書類に付加するための電子署名生成手段と、電子書類に付加された電子署名を抽出し、第２の演算を行なって復号化して個人の認証を行なうための個人認証手段とを含む。

【００１３】

電子署名生成手段は、第１の情報に対して、本人の身体に関連した情報を数値化して得られた独自情報を用いて第１の演算を行なって暗号化された電子署名を生成するので、本人の特定が困難となり、電子署名が偽造されて悪用されることを防止することが可能となる。したがって、市場における個人のプライバシおよびプロパティを守ることが可能となる。

【００１４】

請求項２に記載の認証装置は、請求項１記載の認証装置であって、電子署名生成手段は、本人の独自情報を暗号化して独自ビット情報を生成するための独自ビット情報化手段と、第１の情報に対して、独自ビット情報化手段によって生成された独自ビット情報を用いて論理演算して暗号化するための論理演算手段と、論

理演算手段によって暗号化された情報を電子署名として電子書類に付加するための電子署名付加手段とを含む。

【００１５】

独自ビット情報化手段は、本人の独自情報を暗号化して独自ビット情報を生成するので、本人を特定することがさらに困難となり、サインの偽造の防止をさらに的確に行なうことが可能となる。

【００１６】

請求項３に記載の認証装置は、請求項１または２記載の認証装置であって、個人認証手段は、電子書類に付加された電子署名を抽出するための抽出手段と、抽出手段によって抽出された電子署名に対して、独自ビット情報化手段によって生成された独自ビット情報を用いて論理逆演算を行なって第２の情報を生成するための論理逆演算手段と、第１の情報と、論理逆演算手段によって生成された第２の情報とを比較して、個人の認証を行なうための比較手段とを含む。

【００１７】

比較手段は、第１の情報と、論理逆演算手段によって生成された第２の情報とを比較して、個人の認証を行なうので、電子署名が偽造されたものであるか否かを容易に判定することが可能となる。

【００１８】

請求項４に記載の認証装置は、カードによる支払い時に本人の確認を行なう認証装置であって、第１の情報に対して、本人の独自情報を用いて論理演算を行なって、暗号化された認識情報を生成するための認識情報生成手段と、カードに予め記録された認識情報と、認識情報生成手段によって生成された認識情報とを比較して本人の確認を行なうための認証手段とを含む。

【００１９】

認証手段は、カードに予め記録された認識情報と、認識情報生成手段によって生成された認識情報とを比較して本人の確認を行なうので、本人の確認が容易に行なえるようになる。また、カードに本人を特定するための情報を付加しないようにすると、カードの所有者を容易に特定することが困難となり、カードが悪用される可能性が低くなる。

【００２０】

請求項５に記載の認証装置は、請求項４記載の認証装置であって、認識情報生成手段は、本人の独自情報を暗号化して独自ビット情報を生成するための独自ビット情報化手段と、第１の情報に対して、独自ビット情報化手段によって生成された独自ビット情報を用いて論理演算を行なって、認識情報を生成するための論理演算手段とを含む。

【００２１】

独自ビット情報化手段は、本人の独自情報を暗号化して独自ビット情報を生成するので、本人を特定することがさらに困難となり、カードの偽造等の防止をさらに的確に行なうことが可能となる。

【００２２】

請求項６に記載の認証装置は、請求項５記載の認証装置であって、さらにカードに予め記録された認識情報に対して、独自ビット情報化手段によって生成された独自ビット情報を用いて論理逆演算を行なって第２の情報を生成するための論理逆演算手段と、第１の情報と論理逆演算手段によって生成された第２の情報とを比較して、個人の認証を行なうための比較手段とを含む。

【００２３】

比較手段は、第１の情報と論理逆演算手段によって生成された第２の情報とを比較して、個人の認証を行なうので、カードによる支払いの正当性を認証することが可能となる。

【００２４】

請求項７に記載の認証装置は、請求項４～６のいずれかに記載の認証装置であって、独自情報は、本人の身体に関連した情報を数値化して得られた情報である。

【００２５】

したがって、本人を特定することがさらに困難となり、カードが偽造されて悪用されることを防止することが可能となる。

【００２６】

請求項８に記載の照合装置は、カードによる支払い時に手書きのサインによっ

て本人の確認を行なう照合装置であって、カードに記録された認識情報に対して、暗号鍵を用いて論理演算を行なって第１のサイン情報を生成するための論理演算手段と、論理演算手段によって生成された第１のサイン情報と、手書きのサインを数値化して得られた第２のサイン情報とを比較して本人であるかを検証するための一致検証手段とを含む。

【００２７】

一致検証手段は、論理演算手段によって生成された第１のサイン情報と、手書きのサインを数値化して得られた第２のサイン情報とを比較して本人であるかを検証するので、本人の確認を容易に行なうことが可能となる。

【００２８】

請求項９に記載の照合装置は、請求項８記載の照合装置であって、認識情報は、第１の情報に対して、本人の独自情報を暗号化して生成された独自ビット情報を用いて論理演算を行なった情報である。

【００２９】

したがって、本人を特定することがさらに困難となり、サインの偽造の防止をさらに的確に行なうことが可能となる。

【００３０】

請求項１０に記載の照合装置は、請求項８または９記載の照合装置であって、独自情報は、本人の身体に関連した情報を数値化して得られた情報である。

【００３１】

したがって、本人を特定することがさらに困難となり、カードが偽造されて悪用されることを防止することが可能となる。

【００３２】

請求項１１に記載の電子認証システムは、カードによる支払い時に手書きのサインによって本人の確認を行なう照合装置と、支払いの正当性を認証する認証装置とを接続した電子認証システムであって、認証装置は、本人の独自情報を暗号化して独自ビット情報を生成するための独自ビット情報化手段と、第１の情報に対して、独自ビット情報化手段によって生成された独自ビット情報を用いて論理演算を行なって、認識情報を生成するための第１の論理演算手段と、手書きサイ

ンを数値化して得られた第１のサイン情報に対して、第１の論理演算手段によって生成された認識情報を用いて論理演算を行なって、暗号鍵を生成するための暗号キー化手段と、照合装置から伝送された情報から暗証番号を抽出するための暗証番号抽出手段と、暗証番号抽出手段によって抽出された暗証番号に対して、独自ビット情報化手段によって生成された独自ビット情報を用いて論理逆演算を行なって、第２の情報を生成するための論理逆演算手段と、第１の情報と、論理逆演算手段によって生成された第２の情報とを比較して支払いの正当性の認証を行なうための比較手段とを含み、照合装置は、カードに記録された認識情報に対して、暗号キー化手段によって生成された暗号鍵を用いて論理演算を行なって、第２のサイン情報を生成するための第２の論理演算手段と、第２の論理演算手段によって生成された第２のサイン情報と、手書きのサインを数値化して得られた第３のサイン情報とを比較して本人であるかを検証するための一致検証手段とを含む。

【００３３】

一致検証手段は、第２の論理演算手段によって生成された第２のサイン情報と、手書きのサインを数値化して得られた第３のサイン情報とを比較して本人であるかを検証するので、本人の確認を容易に行なうことが可能となる。また、比較手段は、第１の情報と、論理逆演算手段によって生成された第２の情報とを比較して支払いの正当性の認証を行なうので、カードの偽造等による不正な支払いを発見することが可能となる。さらには、照合装置と認証装置との間の通信を無線通信としたり、ネットワークを介して行なうことによって、リアルタイムで支払いの正当性の認証を行なうことが可能となる。

【００３４】

請求項１２に記載の認証装置は、外部から支払い依頼があった時に本人の確認を行なう認証装置であって、本人の独自情報に対して、時間とともに変化する第１の番号を用いて論理逆演算を行なって、暗号化された暗証番号を生成するための暗証番号生成手段と、外部から受信した情報に対して、暗証番号生成手段によって生成された暗証番号を用いて論理演算を行ない、当該論理演算結果に基づいて本人の一致を検証する検証手段とを含む。

【００３５】

暗証番号生成手段は、本人の独自情報に対して、時間とともに変化する第１の番号を用いて論理逆演算を行なって、暗号化された暗証番号を生成するので、暗証番号が漏洩して悪用される場合があっても、その時点では暗証番号が変化しているので、本人の一致検証において悪用が判明することになる。したがって、本人の確認を正確に行なうことが可能となる。

【００３６】

請求項１３に記載の認証装置は、請求項１２記載の認証装置であって、検証手段は、本人が予め定めたサインデータに対して、本人の独自情報を用いて論理逆演算を行なって生成されたランダム暗証を外部から受信し、ランダム暗証に対して、暗証番号生成手段によって生成された暗証番号を用いて論理演算を行なうための論理演算手段と、外部からサインデータおよび時間とともに変化する第２の番号を受信し、サインデータに対して、第２の番号を用いて論理逆演算を行なうための番号逆演算手段と、論理演算手段による論理演算結果と番号逆演算手段による論理逆演算結果とを比較して、本人の一致を検証する一致検証手段とを含む。

【００３７】

したがって、本人の一致検証をさらに精度良く行なうことが可能となる。

請求項１４に記載の認証装置は、請求項１２または１３記載の認証装置であって、さらに独自情報に対して、暗証番号生成手段によって生成された暗証番号を用いて論理逆演算を行なって、時間とともに変化する第３の番号を生成するための論理逆演算手段と、第２の番号と論理逆演算手段によって生成された第３の番号とを比較して、個人の認証を行なうための比較手段とを含む。

【００３８】

比較手段は、第２の番号と論理逆演算手段によって生成された第３の番号とを比較して、個人の認証を行なうので、支払い依頼の正当性を認証することが可能となる。

【００３９】

請求項１５に記載の認証装置は、請求項１２～１４のいずれかに記載の認証装

置であって、独自情報は、本人の身体に関連した情報を数値化して得られた情報である。

【００４０】

したがって、本人を特定することが困難となり、暗証番号等が漏洩して悪用されることを防止することが可能となる。

【００４１】

【発明の実施の形態】

（実施の形態１）

本発明の実施の形態１における電子認証システムは、会社間の決裁書、ダイレクトメール等の電子化された書類（以下、電子書類と呼ぶ。）に本人署名を付加して配布した後、その電子書類を回収して正当性を確認するものである。この電子認証システムにおいては、主として広告代理店、商社等に設置される認証装置が電子署名の付加および電子書類の認証を行なう。

【００４２】

図１は、本実施の形態における認証装置の概略構成を示す図である。この認証装置は、コンピュータ本体１、グラフィックディスプレイ装置２、ＦＤ（Floppy Disk）４が装着されるＦＤドライブ３、キーボード５、マウス６、ＣＤ－ＲＯＭ（Compact Disc-Read Only Memory）８が装着されるＣＤ－ＲＯＭ装置７、およびネットワーク通信装置９を含む。認証プログラムは、ＦＤ４またはＣＤ－ＲＯＭ８等の記憶媒体によって供給される。認証プログラムはコンピュータ本体１によって実行され、電子署名の付加と電子書類の認証とが行われる。また、認証プログラムは他のコンピュータより通信回線を経由し、コンピュータ本体１に供給されてもよい。

【００４３】

また、コンピュータ本体１は、ＣＰＵ（Central Processing Unit）１０、ＲＯＭ（Read Only Memory）１１、ＲＡＭ（Random Access Memory）１２およびハードディスク１３を含む。ＣＰＵ１０は、グラフィックディスプレイ装置２、磁気テープ装置３、キーボード５、マウス６、ＣＤ－ＲＯＭ装置７、ネットワーク通信装置９、ＲＯＭ１１、ＲＡＭ１２またはハードディスク１３との間でデータ

を入出力しながら処理を行なう。ＦＤ４またはＣＤ－ＲＯＭ８に記録された認証プログラムは、ＣＰＵ１０によりＦＤドライブ３またはＣＤ－ＲＯＭ装置７を介して一旦ハードディスク１３に格納される。ＣＰＵ１０は、ハードディスク１３から適宜認証プログラムをＲＡＭ１２にロードして実行することによって電子署名の付加と電子書類の認証とを行なう。

【００４４】

図２は、本実施の形態における認証装置の機能的構成を示すブロック図である。この認証装置は、電子署名生成部２１と、書類認証部２２とを含む。電子署名生成部２１は、電子書類に署名する本人の独自情報２４を数値配列に変換して暗号化する独自ビット情報化部２１１と、独自ビット情報化部２１１によって暗号化された後の情報（以下、独自ビット情報と呼ぶ。）に本人の元サイン２３を論理演算する論理演算部２１２と、論理演算部２１２によって論理演算された後の情報を本人のサインとして出力するサイン化部２１３と、サイン化部２１３から出力されたサインを電子書類２５に付加する電子署名付加部２１４とを含む。

【００４５】

書類認証部２２は、市場に配布された電子署名が付加された後の電子書類を回収して本人のサインを抽出するサイン抽出部２２１と、サイン抽出部２２１によって抽出されたサインに対して、独自ビット情報化部２１１から出力された独自ビット情報を用いて論理逆演算を行なう論理逆演算部２２２と、論理逆演算部２２２によって論理逆演算された後のデータを格納する逆演算後データ格納部２２３と、逆演算後データ格納部２２３に格納されたデータと本人が保管する元サイン２３とを比較して電子署名の認証を行なう比較部２２４とを含む。

【００４６】

独自情報２４として、たとえば本人の指紋、網膜紋、ＤＮＡ（DeoxyriboNucleic Acid）等の本人の身体に関連する特有の情報が使用される。独自ビット情報化部２１１は、独自情報２４を取得するための機構を有しており、たとえば指紋であれば本人の指紋を光学的に読取った後、その情報を電子化して独自情報２４を数値配列に変換する。そして、独自ビット情報化部２１１は、予め定められた暗号鍵を用いて数値配列に変換された独自情報を暗号化して独自ビット情報を生

成して論理演算部２１２および論理逆演算部２２２へ出力する。この独自ビット情報は、暗号化鍵として用いられる。

【００４７】

論理演算部２１２は、本人から取得した元サイン２３に対して、独自ビット情報化部２１１から出力された独自ビット情報を用いて論理演算を行なう。元サイン２３は、本人の手書きサインという意味ではなく、たとえば暗証番号等の本人が予め決めて機密事項として保持されるデータを意味するものとする。そして、サイン化部２１３は、論理演算部２１２から出力された論理演算された後のデータをサインとして電子署名付加部２１４へ出力する。

【００４８】

電子署名付加部２１４は、サイン化部２１３から出力されたサインを電子書類２５に付加する。そして、このサインが付加された後の電子書類は、市場に配布されて活用される。なお、サイン化部２１３から出力されるサインを本人に返し、本人が電子書類にサインを付加して市場に配布するようにしても良い。

【００４９】

配布された電子書類が回収されると、その電子書類が偽造されたものでないこと確認するため、電子署名の認証が行なわれる。サイン抽出部２２１は、回収された電子書類からサインを抽出する。このサインは、予め定められた箇所に埋め込まれているため、サイン抽出部２２１がその箇所からデータを読出すことによってサインを抽出する。

【００５０】

論理逆演算部２２２は、サイン抽出部２２１によって抽出されたサインに対して、独自ビット情報を用いて論理逆演算を行ない、元サインを生成して逆演算後データ格納部２２３に格納する。そして、比較部２２４は、本人が保持する元サイン２３と、逆演算後データ格納部２２３に格納される元サインとを比較することによって電子署名の認証を行なう。その結果、本人が署名した電子書類であるか否かが判断可能となる。

【００５１】

以上説明したように、本実施の形態における電子認証システムによれば、本人

特有の情報を数値配列に変換して暗号鍵を生成し、これを用いて元サイン２３を暗号化するようにした。したがって、従来容易に本人を特定してサインを偽造することが可能であったが、本実施の形態における電子認証システムにおいては本人の特定が困難となるため、サインの偽造を防止することが可能となった。それによって、市場における個人のプライバシおよびプロパティを守ることが可能となった。

【００５２】

（実施の形態２）

本発明の実施の形態２における電子認証システムは、クレジットカード等のカードを使用して店頭で商品の購入等を行なう際に本人の確認を行ない、後日支払いの正当性を確認するために個人の認証を行なうものである。この電子認証システムにおいては、主としてカードによる支払いが行なわれる店舗等に設置された認証装置が、支払現場における本人の確認および後日支払いの正当性確認のための認証とを行なう。なお、カードには、本人の手書きのサイン、顔写真等の本人を特定するための情報が付加されておらず、カードの所有者を容易に特定することができないものとする。したがって、カードを紛失したり、盗難に遭った場合であっても、カードの持ち主を特定することができないため、悪用される可能性が低くなる。また、後述するようにカードに独自ビット情報から生成された情報が記録されているため、このカードを偽造することが極めて困難となる。

【００５３】

本実施の形態における認証装置は、図１に示す実施の形態１における認証装置の概略構成と同じである。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００５４】

図３は、本実施の形態における認証装置の機能的構成を示すブロック図である。この認証装置は、支払時個人認証部３１と、後日個人認証部３２とを含む。支払時個人認証部３１は、カードを使用する本人の独自情報３４を数値配列に変換して暗号化する独自ビット情報化部３１１と、本人の暗証番号３３に対して、独自ビット情報化部３１１によって生成された独自ビット情報を用いて論理演算を

行なう論理演算部３１２と、論理演算部３１２によって論理演算された後の情報を本人の認識情報として出力する認識情報化部３１３と、認識情報化部３１３から出力された認識情報とクレジットカードに格納された認識情報とを比較して支払い現場における認証を行なうとともに、カードから読取った認識情報を含んだ情報をカード会社へ伝送する認証部３１４とを含む。

【００５５】

後日個人認証部３２は、カード会社からの確認依頼を受けて、カード会社から伝送される情報から認識情報を抽出する認識情報抽出部３２１と、認識情報抽出部３２１によって抽出された認識情報に対して、独自ビット情報化部３１１から出力された独自ビット情報を用いて論理逆演算を行なう論理逆演算部３２２と、論理逆演算部３２２によって論理逆演算された後のデータを格納する逆演算後データ格納部３２３と逆演算後データ格納部３２３に格納されたデータと本人が保持する暗証番号３３とを比較して個人の認証を行なう比較部３２４とを含む。

【００５６】

独自情報３４として、実施の形態１と同様に、本人の身体に関連する特有の情報が使用される。独自ビット情報化部３１１は、予め定められた暗号鍵を用いて数値配列に変換された独自情報を暗号化して独自ビット情報を生成して論理演算部３１２および論理逆演算部３２２へ出力する。この独自ビット情報は、暗号化鍵として用いられる。

【００５７】

論理演算部３１２は、本人から取得した暗証番号に対して、独自ビット情報化部３１１から出力された独自ビット情報を用いて論理演算を行なう。そして、認識情報化部３１３は、論理演算部３１２から出力された論理演算された後のデータを認識情報として認証部３１４へ出力する。この認識情報は、本人が有するカードにも予め記録されている。

【００５８】

認証部３１４は、支払い現場において商品の購入者等から提示されたカードに記録された情報を読取るための機構、たとえばカードリーダを有しており、カードから読取った情報に含まれる認識情報と認識情報化部３１３から出力される認

識情報とを比較してカードの認証を行なう。このとき、支払い現場において商品の購入者等が本人を特定する情報、たとえば氏名等を提示する。認証部３１４は、提示された本人の氏名等に基づいて認識情報を選択して認証を行なう。

【００５９】

支払い現場における認証が終了して、クレジットカードによる支払いが終了した後、認証部３１４はカードから読取られた認識情報および支払いが行なわれた商品の識別情報等をカード会社へ伝送して、伺いを立てる。

【００６０】

また、後日カード会社から認証の確認依頼があれば、支払いの正当性を確認するための認証が行なわれる。認識情報抽出部３２１は、カード会社から伝送された情報の中から認識情報を抽出して論理逆演算部３２２へ出力する。論理逆演算部３２２は、認識情報抽出部３２１によって抽出された認識情報に対して、独自ビット情報を用いて論理逆演算を行ない、暗証番号を生成して逆演算後データ格納部３２３に格納する。そして、比較部３２４は、本人が保持する暗証番号３３と、逆演算後データ格納部３２３に格納される暗証番号とを比較することによって支払いの正当性の確認を行ない、その確認結果がカード会社へ連絡される。その結果、本人がカードを用いて支払いを行なったか否かが判断可能となる。

【００６１】

本実施の形態においては、カードに認識情報を格納して認証を行なう場合について説明したが、携帯情報端末が認識情報を保持し、認証装置に携帯情報端末を接続して支払いの認証を行なうようにしても良い。また、認証装置がカード会社以外の会社等に設置される場合について説明したが、カード会社に認証装置が設置される場合には、認識情報抽出部３２１はカードから読取られた情報から直接認識情報を抽出する。この場合、認識情報が漏洩する可能性がさらに低くなり、本人確認の信頼性をさらに高めることが可能となる。

【００６２】

以上説明したように、本実施の形態における電子認証システムによれば、本人特有の情報を数値配列に変換して暗号鍵を生成し、これを用いて暗証番号３３を暗号化して認証を行なうようにした。したがって、カードを紛失したり、盗難に

遭った場合であっても本人の特定が困難であるため、カードが不正に使用されることを防止することが可能となった。

【００６３】

（実施の形態３）

本発明の実施の形態３における電子認証システムは、カードを使用して店頭で商品の購入等を行なう際に本人の確認を行ない、リアルタイムで支払いの正当性を確認するために個人の認証を行なうものである。この電子認証システムにおいては、カードによる支払いが行なわれる店舗等に設置された端末装置がカードに格納された認識情報を読取って、カード会社を経由してクレジット会社に設置された認証装置へ伝送し、この認証装置が支払現場における本人の認証および支払いの正当性の確認をリアルタイムで行なう。なお、実施の形態２と同様に、カードには、本人の手書きのサイン、顔写真等の本人を特定するための情報が付加されておらず、カードの所有者を容易に特定することができないものとする。したがって、カードを紛失したり、盗難に遭った場合であっても、カードの持ち主を特定することができないため、悪用される可能性が低くなる。また、後述するようにカードに独自ビット情報から生成された情報が記録されているため、このカードを偽造することが極めて困難となる。

【００６４】

本実施の形態における認証装置は、図１に示す実施の形態１における認証装置の概略構成と同じである。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００６５】

図４は、本実施の形態における認証装置の機能的構成を示すブロック図である。この認証装置は、認識情報生成部４１と、個人認証部４２とを含む。認識情報生成部４１は、カードを使用する本人の独自情報４４を数値配列に変換して暗号化する独自ビット情報化部４１１と、本人の暗証番号４３に対して、独自ビット情報化部４１１によって生成された独自ビット情報を用いて論理演算を行なう論理演算部４１２と、論理演算部４１２によって論理演算された後の情報を本人の認識情報として出力する認識情報化部４１３とを含む。

【００６６】

個人認証部４２は、カード会社からの確認依頼を受けて、カード会社から伝送される情報から認識情報を抽出する認識情報抽出部４２１と、認識情報抽出部４２１によって抽出された認識情報に対して、独自ビット情報化部４１１から出力された独自ビット情報を用いて論理逆演算を行なう論理逆演算部４２２と、論理逆演算部４２２によって論理逆演算された後のデータを格納する逆演算後データ格納部４２３と、逆演算後データ格納部４２３に格納されたデータと本人が保持する暗証番号４３とを比較して個人の認証を行なう比較部４２４とを含む。

【００６７】

独自情報４４として、実施の形態１と同様に、本人の身体に関連する特有の情報が使用される。独自ビット情報化部４１１は、予め定めされた暗号鍵を用いて数値配列に変換された独自情報を暗号化して独自ビット情報を生成して論理演算部４１２および論理逆演算部４２２へ出力する。この独自ビット情報は、暗号化鍵として用いられる。

【００６８】

論理演算部４１２は、本人から取得した暗証番号に対して、独自ビット情報化部４１１から出力された独自ビット情報を用いて論理演算を行なう。そして、認識情報化部４１３は、論理演算部４１２から出力された論理演算された後のデータを認識情報として出力する。この認識情報は、本人が有するカードに予め記録されている。

【００６９】

店舗等の支払現場に設置された端末装置は、カードリーダ等のカードを読取る機構を有しており、商品の購入者等が提示したカードに格納されている認識情報を含んだ情報を読出して、ネットワーク、無線通信等によってカード会社に認識情報を含んだ情報を伝送して伺いを立てる。なお、端末装置の概略構成は、図１に示す実施の形態１における認証装置の概略構成と比較して、カードリーダが接続されている点を除いて同様であるので、詳細な説明は繰返さない。

【００７０】

カード会社は端末装置から情報を受信すると、その情報をネットワーク、無線

通信等によって認証装置へ伝送する。認識情報抽出部４２１は、カード会社から伝送された情報の中から認識情報を抽出して論理逆演算部４２２へ出力する。論理逆演算部４２２は、認識情報抽出部４２１によって抽出された認識情報に対して、独自ビット情報を用いて論理逆演算を行ない、暗証番号を生成して逆演算後データ格納部４２３に格納する。

【００７１】

比較部４２４は、本人が提示する暗証番号４３と、逆演算後データ格納部４２３に格納される暗証番号とを比較することによって支払いの正当性の確認を行ない、その確認結果がカード会社へ連絡される。そして、カード会社は認証結果を支払い現場に設置された端末装置へ伝送する。その結果、本人がカードを用いて支払いを行なったか否かが判断可能となる。

【００７２】

本実施の形態においては、カードに認識情報を格納して認証を行なう場合について説明したが、携帯情報端末が認識情報を保持し、端末装置に携帯情報端末を接続して支払いの認証を行なうようにしても良い。また、認証装置がカード会社以外の会社等に設置される場合について説明したが、カード会社に認証装置が設置される場合には、認識情報抽出部４２１はカードから読取られた情報から直接認識情報を抽出する。この場合、認識情報が漏洩する可能性がさらに低くなり、本人確認の信頼性をさらに高めることが可能となる。

【００７３】

以上説明したように、本実施の形態における電子認証システムによれば、本人特有の情報を数値配列に変換して暗号鍵を生成し、これを用いて暗証番号４３を暗号化して認証を行なうようにした。したがって、カードを紛失したり、盗難に遭った場合であっても本人の特定が困難であるため、カードが不正に使用されることを防止することが可能となった。また、支払い現場において読取られた認識情報がネットワーク、無線通信等によってリアルタイムに認証装置へ伝送され、認証結果もリアルタイムで支払い現場へ伝送されるため、支払いの正当性の確認を支払い現場において行なうことが可能となった。

【００７４】

（実施の形態４）

本発明の実施の形態４における電子認証システムは、クレジットカード等のカードを使用して店頭で商品の購入等を行なう際に本人の確認を行ない、後日支払いの正当性を確認するために個人の認証を行なうものである。この電子認証システムにおいては、カードによる支払いが行なわれる店舗等に設置された照合装置が、カードに記録された情報から生成されたサインと手書きのサインとを比較して本人の確認を行なう。また、クレジット会社等に設置された認証装置が、後日支払いの正当性確認のための認証を行なう。なお、カードには、本人の手書きのサイン、顔写真等の本人を特定するための情報が付加されておらず、カードの所有者を容易に特定することができないものとする。したがって、カードを紛失したり、盗難に遭った場合であっても、カードの持ち主を特定することができないため、悪用される可能性が低くなる。また、後述するようにカードに独自ビット情報から生成された情報が記録されているため、このカードを偽造することが極めて困難となる。

【００７５】

本実施の形態における認証装置は、図１に示す実施の形態１における認証装置の概略構成と同じである。また、本実施の形態における照合装置は、図１に示す実施の形態１における認証装置の概略構成と比較して、手書きのサインを光学的に読取って電子化する機構と、カードに記録された情報を読取るカードリーダ等の機構とを含んでいる点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００７６】

図５は、本実施の形態における照合装置および認証装置の機能的構成を示すブロック図である。照合装置５３は、カードから読取られた情報に対して、暗号キーを用いて論理演算を行なう論理演算部５３１と、手書きのサインを電子化して生成された情報と論理演算部５３１によって論理演算された後の情報とを比較して本人の確認を行なう一致検証部５３２とを含む。

【００７７】

認証装置は、暗号キー生成部５１と、後日個人認証部５２とを含む。暗号キー

生成部５１は、カードを使用する本人の独自情報５５を数値配列に変換して暗号化する独自ビット情報化部５１１と、本人の元番号５４に対して、独自ビット情報化部５１１によって生成された独自ビット情報を用いて論理演算を行なう論理演算部５１２と、本人のサイン５６に対して、論理演算部５１２によって論理演算された後の情報を用いて論理演算を行なって暗号キーを生成する暗号キー化部５１３とを含む。

【００７８】

後日個人認証部５２は、カード会社からの確認依頼を受けて、カード会社から伝送される情報から暗証番号を抽出する暗証番号抽出部５２１と、暗証番号抽出部５２１によって抽出された暗証番号に対して、独自ビット情報化部５１１から出力された独自ビット情報を用いて論理逆演算を行なう論理逆演算部５２２と、論理逆演算部５２２によって論理逆演算された後のデータを格納する逆演算後データ格納部５２３と、逆演算後データ格納部５２３に格納されたデータと本人が保持する元番号５４とを比較して個人の認証を行なう比較部５２４とを含む。

【００７９】

独自情報５５として、実施の形態１と同様に、本人の身体に関連する特有の情報が使用される。独自ビット情報化部５１１は、予め定めされた暗号鍵を用いて数値配列に変換された独自情報を暗号化して独自ビット情報を生成して論理演算部５１２および論理逆演算部５２２へ出力する。この独自ビット情報は、暗号化鍵として用いられる。

【００８０】

論理演算部５１２は、本人から取得した元番号（Ｂ）に対して、独自ビット情報化部５１１から出力された独自ビット情報（Ａ）を用いて論理演算を行なう。そして、認識情報化部５１３は、論理演算部５１２から出力された論理演算された後のデータ（Ｃ＝Ａ×Ｂ）を暗証番号として暗号キー化部５１３へ出力する。この暗証番号は、本人が有するカードにも予め記録されている。暗号化のための論理演算は、簡単のために乗算（×）のみを行なうものとする。

【００８１】

暗号キー化部５１３は、本人が手書きしたサイン（Ｄ）に対して、論理演算部

５１２から出力された暗証番号（Ｃ）を用いてさらに論理逆演算を行なう。そして、暗号キー化部５１３は、論理逆演算結果（Ｅ＝Ｄ÷Ｃ）を暗号キーとして支払い現場に設置された照合装置へ伝送する。

【００８２】

支払い現場に設置された照合装置は、商品の購入者等から提示されたカードから暗証番号（Ｃ）を読取るとともに、商品の購入者等が手書きしたサインを光学的に読取って電子化された情報（Ｄ’）に変換する。論理演算部５３１は、読取られた暗証番号（Ｃ）に対して、暗号キー化部５１３から出力された暗号キー（Ｅ）を用いて論理演算を行なう。論理演算部５３１は、その論理演算結果（Ｄ＝Ｃ×Ｅ）を一致検証部５３２へ出力する。

【００８３】

一致検証部５３２は、論理演算部５３１から出力された論理演算結果（Ｄ）と手書きサインが電子化された情報（Ｄ’）とを比較して本人の確認を行なう。支払い現場における本人の確認が終了して、クレジットカードによる支払いが終了した後、照合装置は暗証番号および支払いが行なわれた商品の識別情報等をカード会社へ伝送して、伺いを立てる。

【００８４】

また、後日カード会社から認証の確認依頼があれば、支払いの正当性を確認するための認証が行なわれる。暗証番号抽出部５２１は、カード会社から伝送された情報の中から暗証番号を抽出して論理逆演算部５２２へ出力する。論理逆演算部５２２は、暗証番号抽出部５２１によって抽出された暗証番号に対して、独自ビット情報を用いて論理逆演算を行ない、元番号を生成して逆演算後データ格納部５２３に格納する。そして、比較部５２４は、本人が保持する元番号５４と、逆演算後データ格納部５２３に格納される元番号とを比較することによって支払いの正当性の確認を行ない、その確認結果がカード会社へ連絡される。その結果、本人がカードを用いて支払いを行なったか否かが判断可能となる。

【００８５】

本実施の形態においては、カードに認識情報を格納して認証を行なう場合について説明したが、携帯情報端末が認識情報を保持し、照合装置に携帯情報端末を

接続して支払いの認証を行なうようにしても良い。また、認証装置がカード会社以外の会社等に設置される場合について説明したが、カード会社に認証装置が設置される場合には、暗証番号抽出部５２１はカードから読取られた情報から直接認識情報を抽出する。この場合、認識情報が漏洩する可能性がさらに低くなり、本人確認の信頼性をさらに高めることが可能となる。

【００８６】

以上説明したように、本実施の形態における電子認証システムによれば、本人特有の情報を数値配列に変換して暗号鍵を生成し、これを用いて元番号５４を暗号化して暗証番号を生成し、さらに暗証番号を用いて手書きのサインを暗号化して認証を行なうようにした。したがって、カードを紛失したり、盗難に遭った場合であっても本人の特定が困難であるため、カードが不正に使用されることを防止することが可能となった。また、商品の購入者等が手書きしたサインと、演算して生成されたサインとを比較して本人の確認を行なうようにしたので、支払い現場における本人の確認をさらに正確に行なうことが可能となった。

【００８７】

（実施の形態５）

本発明の実施の形態５における電子認証システムは、インターネット等のデータ通信ネットワークに接続された端末装置を用いて商品の購入等を行なう際に本人の確認を行ない、後日またはリアルタイムで支払いの正当性を確認するために個人の認証を行なうものである。この電子認証システムにおいては、主としてインターネットに接続された認証装置が、本人の確認および支払いの正当性確認のための認証を行なう。

【００８８】

本実施の形態における認証装置は、図１に示す実施の形態１における認証装置の概略構成と同じである。したがって、重複する構成および機能の詳細な説明は繰返さない。

【００８９】

図６は、本実施の形態における認証装置の機能的構成を示すブロック図である。この認証装置は、支払時個人認証部６１と、後日個人認証部６２とを含む。支

払時個人認証部６１は、カードを使用する本人の独自情報６３を数値配列に変換する独自ビット情報化部６１１と、独自ビット情報化部６１１によって生成された独自ビット情報に対して、時間と共に変化する番号を用いて論理逆演算を行なう論理逆演算部６１２と、論理逆演算部６１２によって論理逆演算された後の情報を暗証番号として出力する暗証番号化部６１３と、端末装置から伝送されたサインデータに対して番号を用いて論理逆演算を行なう番号逆演算部６１４と、端末装置から伝送されたランダム暗証に対して、暗証番号化部６１３から出力された暗証番号を用いて論理演算する論理演算部６１５と、番号逆演算部６１４から出力された論理逆演算結果と論理演算部６１５から出力された論理演算結果とを比較して本人の確認を行なう一致検証部６１６とを含む。

【００９０】

後日個人認証部６２は、カード会社からの確認依頼を受けて、カード会社から伝送される情報から暗証番号を抽出する暗証番号抽出部６２１と、独自ビット情報化部６１１から出力された独自ビット情報に対して、暗証番号抽出部６２１によって抽出された暗証番号を用いて論理逆演算を行なう論理逆演算部６２２と、論理逆演算部６２２によって論理逆演算された後のデータを格納する逆演算後データ格納部６２３と、逆演算後データ格納部６２３に格納されたデータと本人が保持する番号６４とを比較して個人の認証を行なう比較部６２４とを含む。

【００９１】

端末装置を使用して商品等を購入する利用者と、認証装置が設置されるサービス会社との間で、予め元番号およびパスワードが決められており、端末装置および認証装置に元番号およびパスワードが予め登録されているものとする。このパスワードは、利用者を特定する情報として使用される。また、利用者は予めサインデータ６６を決めており、端末装置に登録されているものとする。

【００９２】

認証装置および端末装置は、標準時間が重畳された電波を受信する機構を有しており、標準時間を用いて情報を暗号化する。ここでは簡単のために、標準時間を時間暗号と呼ぶことにし、所定の情報に時間暗号を乗算して所定の情報を暗号化することにする。したがって、認証装置および端末装置で生成される番号は時

間とともに変化するが、互いに同期が取れており、常に同じ番号を生成することができる。時間とともに変化する番号は、以下の式によって表わされる。

【００９３】

番号＝元番号／時間暗号　　…（１）

独自情報６３として、実施の形態１と同様に、本人の身体に関連する特有の情報が使用される。独自ビット情報化部６１１は、独自情報６３を数値配列に変換し独自ビット情報を生成して論理逆演算部６１２および論理逆演算部６２２へ出力する。この独自ビット情報は、暗号化鍵として用いられる。

【００９４】

論理逆演算部６１２は、独自ビット情報化部６１１から出力された独自ビット情報に対して、登録された元番号を用いて論理逆演算を行なう。そして、暗証番号化部６１３は、論理逆演算部６１２から出力された論理逆演算された後のデータに対して、時間暗号を論理演算することにより暗証番号を生成して論理演算部６１５へ出力する。したがって、暗証番号は、次式によって表わされる。

【００９５】

暗証番号＝独自ビット情報／番号

＝独自ビット情報×時間暗号／元番号　　…（２）

一方、端末装置において、サインデータ６６および独自ビット情報を用いてランダム暗証を算出する。このランダム暗証は、次式によって表わされる。

【００９６】

ランダム暗証＝サインデータ／独自ビット情報　　…（３）

利用者によって商品の購入等が行なわれて支払い依頼６５があると、端末装置から認証装置へサインデータ６６、番号６４、ランダム暗証およびパスワードが伝送される。番号逆演算部６１４は、サインデータ６６に対して、番号６４を用いて論理逆演算を行なう。また、論理演算部６１５は、ランダム暗証に対して、パスワードによって選択された独自ビット情報を用いて論理演算を行なう。そして、一致検証部６１６は、番号逆演算部６１４から出力された論理逆演算結果と、論理演算部６１５から出力された論理演算結果とを比較して、本人の確認を行なう。したがって、次式によって認証が行なわれることになる。

【００９７】

ランダム暗証×暗証番号＝サインデータ／番号　　…（４）

また、（４）式は次式によって表わすこともできる。

【００９８】

ランダム暗証×暗証番号＝サインデータ×時間暗号／元番号　　…（５）

なお、認証装置と端末装置との間で時刻にずれがある場合には、認証装置が端末装置から支払い時の時刻を取得するようにし、認証装置が保持する時刻とのずれ量を算出して、そのずれ量を補正して時間暗号を求めるようにしても良い。

【００９９】

インターネットを介した支払いが終了した後、認証装置は暗証番号および支払いが行なわれた商品の識別情報等をカード会社へ伝送して、伺いを立てる。

【０１００】

また、後日カード会社から認証の確認依頼があれば、支払いの正当性を確認するための認証が行なわれる。暗証番号抽出部６２１は、カード会社から伝送された情報の中から暗証番号を抽出して論理逆演算部６２２へ出力する。論理逆演算部６２２は、暗証番号抽出部６２１によって抽出された暗証番号に対して、独自ビット情報を用いて論理逆演算を行ない、番号を生成して逆演算後データ格納部６２３に格納する。そして、比較部６２４は、本人が保持する支払い時の番号６４と、逆演算後データ格納部６２３に格納される番号とを比較することによって支払いの正当性の確認を行ない、その確認結果がカード会社へ連絡される。その結果、本人が取引を行なったか否かが判断可能となる。

【０１０１】

本実施の形態においては、認証装置がカード会社以外の会社等に設置される場合について説明したが、カード会社に認証装置が設置される場合には、暗証番号抽出部６２１は暗証番号化部６１３から直接暗証番号を取得する。この場合、暗証番号が漏洩する可能性がさらに低くなり、本人確認の信頼性をさらに高めることが可能となる。

【０１０２】

以上説明したように、本実施の形態における電子認証システムによれば、本人

とサービス会社との間で決めた元番号と時間暗号とから番号を生成し、この時間番号に基づいて情報を暗号化するようにしたので、インターネットを介して暗証番号等が漏洩するのを防止することが可能となった。また、本人特有の情報を数値配列に変換し、これを用いて暗証番号を生成するようにしたので、さらに効果的に暗証番号等の漏洩を防止することが可能となった。

【０１０３】

今回開示された実施の形態は、すべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【０１０４】

【発明の効果】

請求項１に記載の認証装置によれば、電子署名生成手段が第１の情報に対して、本人の身体に関連した情報を数値化して得られた独自情報を用いて第１の演算を行なって暗号化された電子署名を生成するので、本人の特定が困難となり、電子署名が偽造されて悪用されることを防止することが可能となる。したがって、市場における個人のプライバシおよびプロパティを守ることが可能となった。

【０１０５】

請求項２に記載の認証装置によれば、独自ビット情報化手段が本人の独自情報を暗号化して独自ビット情報を生成するので、本人を特定することがさらに困難となり、サインの偽造の防止をさらに的確に行なうことが可能となった。

【０１０６】

請求項３に記載の認証装置によれば、比較手段が第１の情報と、論理逆演算手段によって生成された第２の情報とを比較して、個人の認証を行なうので、電子署名が偽造されたものであるか否かを容易に判定することが可能となった。

【０１０７】

請求項４に記載の認証装置によれば、認証手段がカードに予め記録された認識情報と、認識情報生成手段によって生成された認識情報とを比較して本人の確認を行なうので、本人の確認が容易に行なえるようになった。また、カードに本人

を特定するための情報を付加しないようにすると、カードの所有者を容易に特定することが困難となり、カードが悪用される可能性が低くなる。

【０１０８】

請求項５に記載の認証装置によれば、独自ビット情報化手段が本人の独自情報を暗号化して独自ビット情報を生成するので、本人を特定することがさらに困難となり、カードの偽造等の防止をさらに的確に行なうことが可能となった。

【０１０９】

請求項６に記載の認証装置によれば、比較手段が第１の情報と論理逆演算手段によって生成された第２の情報とを比較して、個人の認証を行なうので、カードによる支払いの正当性を認証することが可能となった。

【０１１０】

請求項７に記載の認証装置によれば、本人を特定することがさらに困難となり、カードが偽造されて悪用されることを防止することが可能となった。

【０１１１】

請求項８に記載の照合装置によれば、一致検証手段が論理演算手段によって生成された第１のサイン情報と、手書きのサインを数値化して得られた第２のサイン情報とを比較して本人であるかを検証するので、本人の確認を容易に行なうことが可能となった。

【０１１２】

請求項９に記載の照合装置によれば、本人を特定することがさらに困難となり、サインの偽造の防止をさらに的確に行なうことが可能となった。

【０１１３】

請求項１０に記載の照合装置によれば、本人を特定することがさらに困難となり、カードが偽造されて悪用されることを防止することが可能となった。

【０１１４】

請求項１１に記載の電子認証システムによれば、一致検証手段が第２の論理演算手段によって生成された第２のサイン情報と、手書きのサインを数値化して得られた第３のサイン情報とを比較して本人であるかを検証するので、本人の確認を容易に行なうことが可能となった。また、比較手段が第１の情報と、論理逆演

算手段によって生成された第２の情報とを比較して支払いの正当性の認証を行なうので、カードの偽造等による不正な支払いを発見することが可能となった。さらには、照合装置と認証装置との間の通信を無線通信としたり、ネットワークを介して行なったりすることによって、リアルタイムで支払いの正当性の認証を行なうことが可能となった。

【０１１５】

請求項１２に記載の認証装置によれば、暗証番号生成手段は、本人の独自情報に対して、時間とともに変化する第１の番号を用いて論理逆演算を行なって、暗号化された暗証番号を生成するので、暗証番号が漏洩して悪用される場合があっても、その時点では暗証番号が変化しているので、本人の一致検証において悪用が判明することになる。したがって、本人の確認を正確に行なうことが可能となった。

【０１１６】

請求項１３に記載の認証装置によれば、本人の一致検証をさらに精度良く行なうことが可能となった。

【０１１７】

請求項１４に記載の認証装置によれば、比較手段が第２の番号と論理逆演算手段によって生成された第３の番号とを比較して、個人の認証を行なうので、支払い依頼の正当性を認証することが可能となった。

【０１１８】

請求項１５に記載の認証装置によれば、本人を特定することが困難となり、暗証番号等が漏洩して悪用されることを防止することが可能となった。

【図面の簡単な説明】

【図１】　本発明の実施の形態１における認証装置の概略構成を示すブロック図である。

【図２】　本発明の実施の形態１における認証装置の機能的構成を説明するための図である。

【図３】　本発明の実施の形態２における認証装置の機能的構成を説明するための図である。

【図４】　本発明の実施の形態３における認証装置の機能的構成を説明するための図である。

【図５】　本発明の実施の形態４における認証装置の機能的構成を説明するための図である。

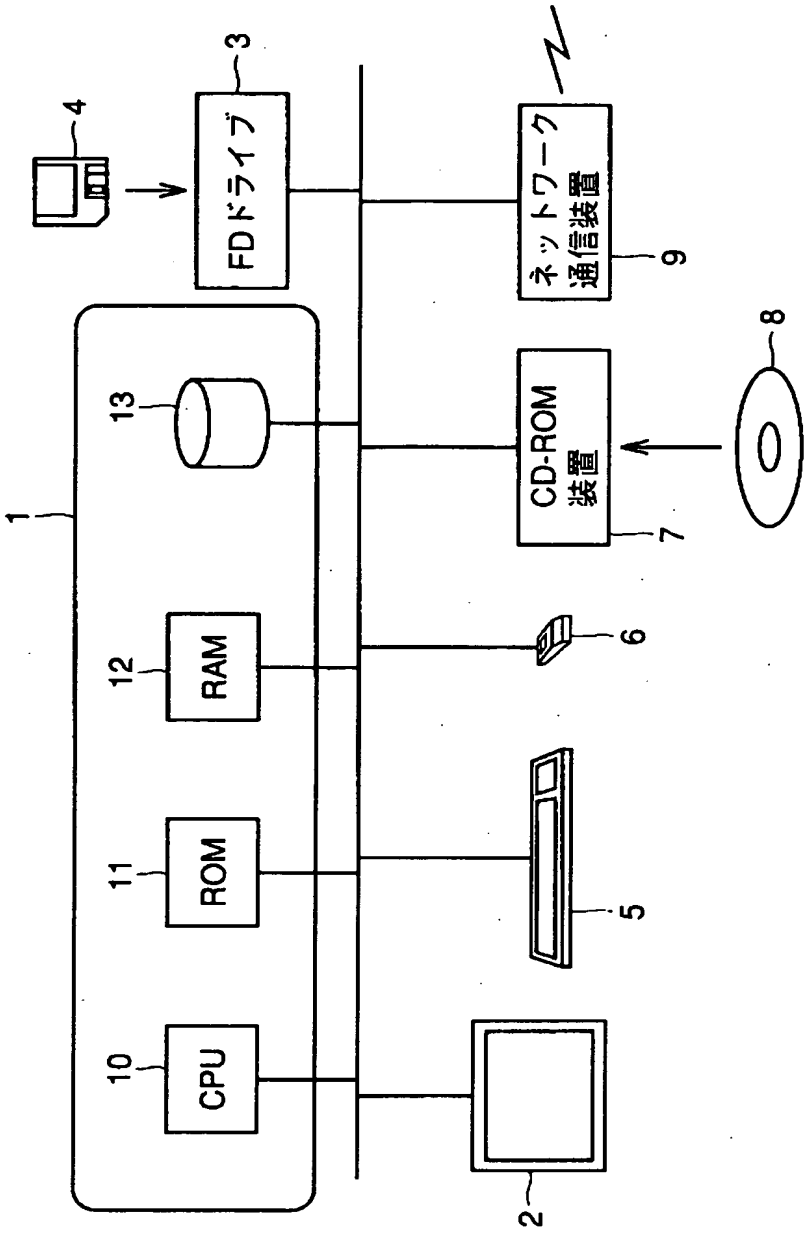
【図６】　本発明の実施の形態５における認証装置の機能的構成を説明するための図である。

【符号の説明】

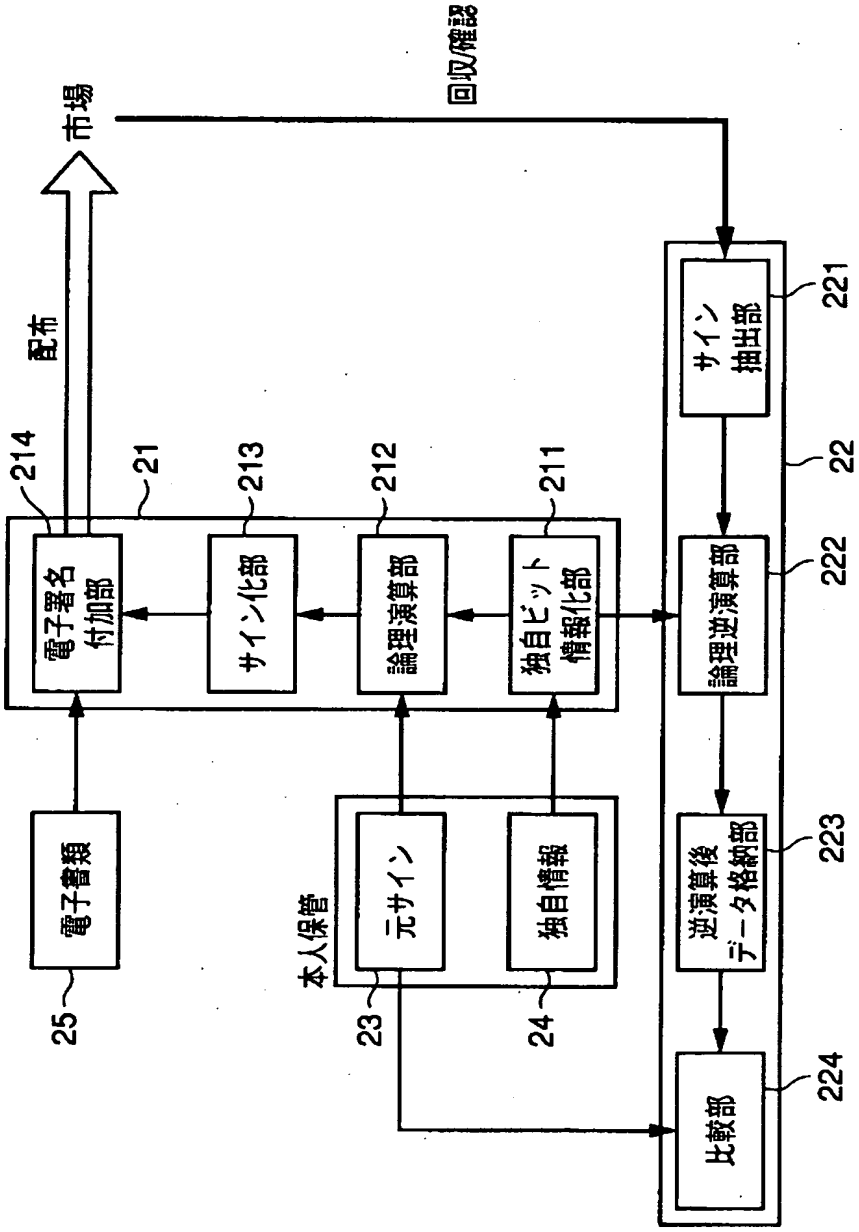
１　コンピュータ本体、２　グラフィックディスプレイ装置、３　ＦＤドライブ、４　ＦＤ、５　キーボード、６　マウス、７　ＣＤ－ＲＯＭ装置、８　ＣＤ－ＲＯＭ、９　ネットワーク通信装置、１０　ＣＰＵ、１１　ＲＯＭ、１２　ＲＡＭ、１３　ハードディスク、２１　電子署名生成部、２２　書類認証部、２３　元サイン、２４，３４，４４，５５，６３　独自情報、２５　電子書類、３１，６１　支払時個人認証部、３２，５２，６２　後日個人認証部、３３，４３　暗証番号、３５，４５，５７，６５　支払い依頼、４１　認識情報生成部、４２　個人認証部、４６　認識情報、５１　暗号キー生成部、５３　照合装置、５４　元番号、５６　サイン、６４　番号、６６　サインデータ、２１１，３１１，４１１，５１１，６１１　独自ビット情報化部、２１２，３１２，４１２，５１２，６１５　論理演算部、２１３　サイン化部、２１４　電子署名付加部、２２１　サイン抽出部、２２２，３２２，４２２，５２２，６１２，６２２　論理逆演算部、２２３，３２３，４２３，５２３，６２３　逆演算後データ格納部、２２４，３２４，４２４，５２４，６２４　比較部、３１３，４１３　認識情報化部、３２１，４２１　認識情報抽出部、５１３　暗号キー化部、５２１，６２１　暗証番号抽出部、６１３　暗証番号化部、６１４　番号逆演算部、６１６　一致検証部。

【書類名】　　図面

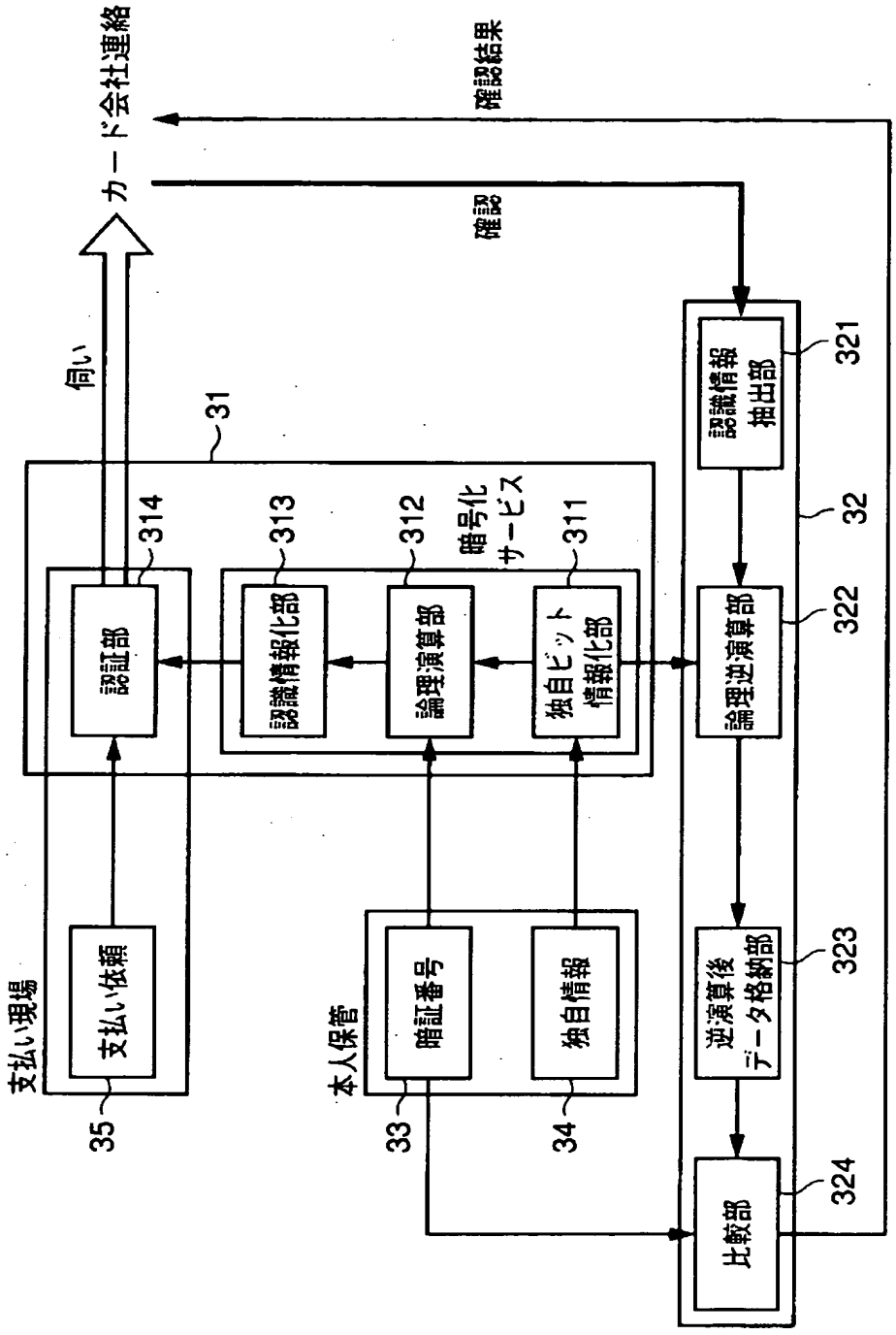
【図１】



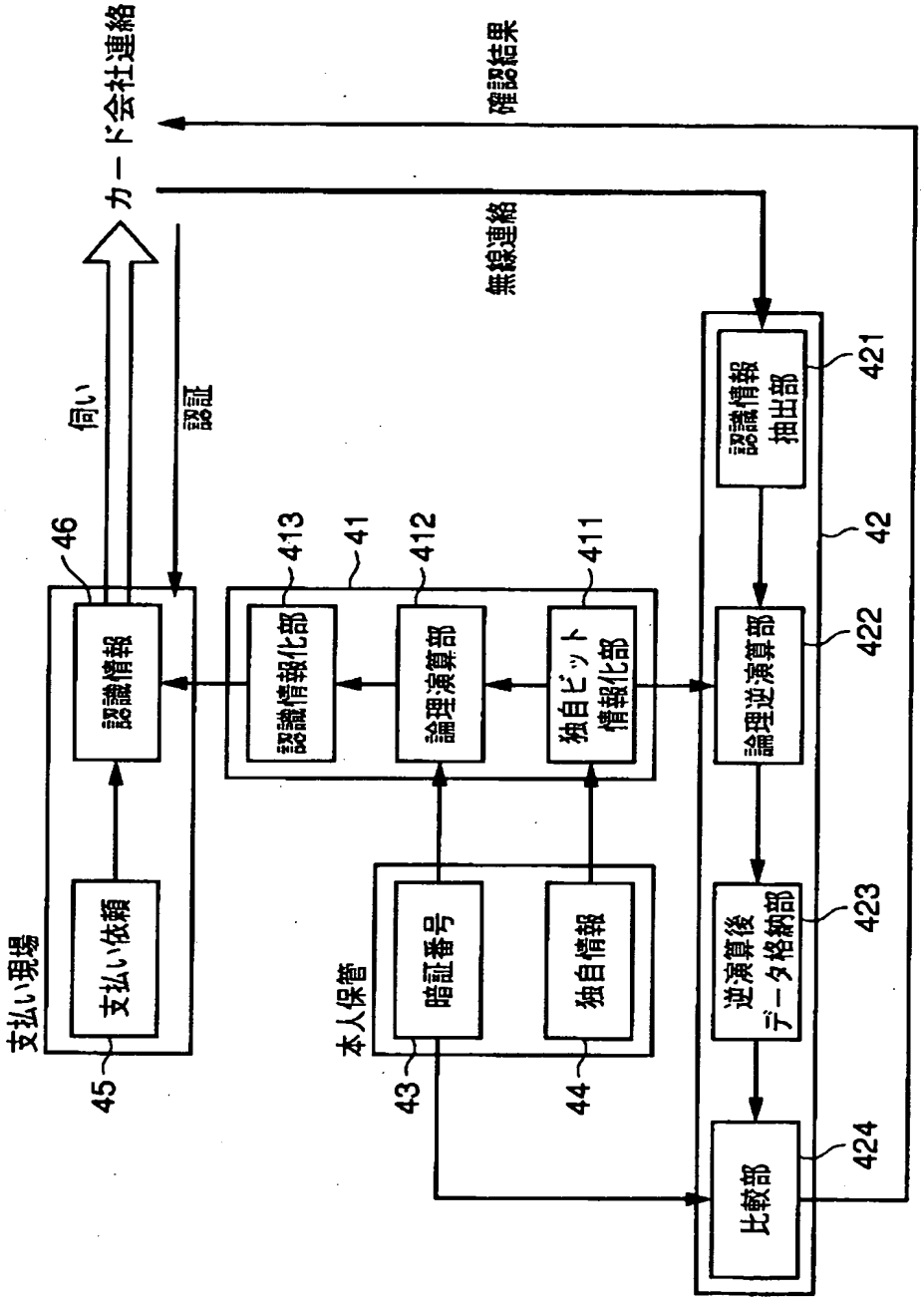
【図２】


回収/確認
市場
配布
214
21
213
212
211
電子署名付加部
サイン化部
論理演算部
独自ビット情報化部
電子書類
25
本人保管
元サイン
独自情報
23
24
221
22
222
223
224
サイン抽出部
論理逆演算部
逆演算後データ格納部
比較部

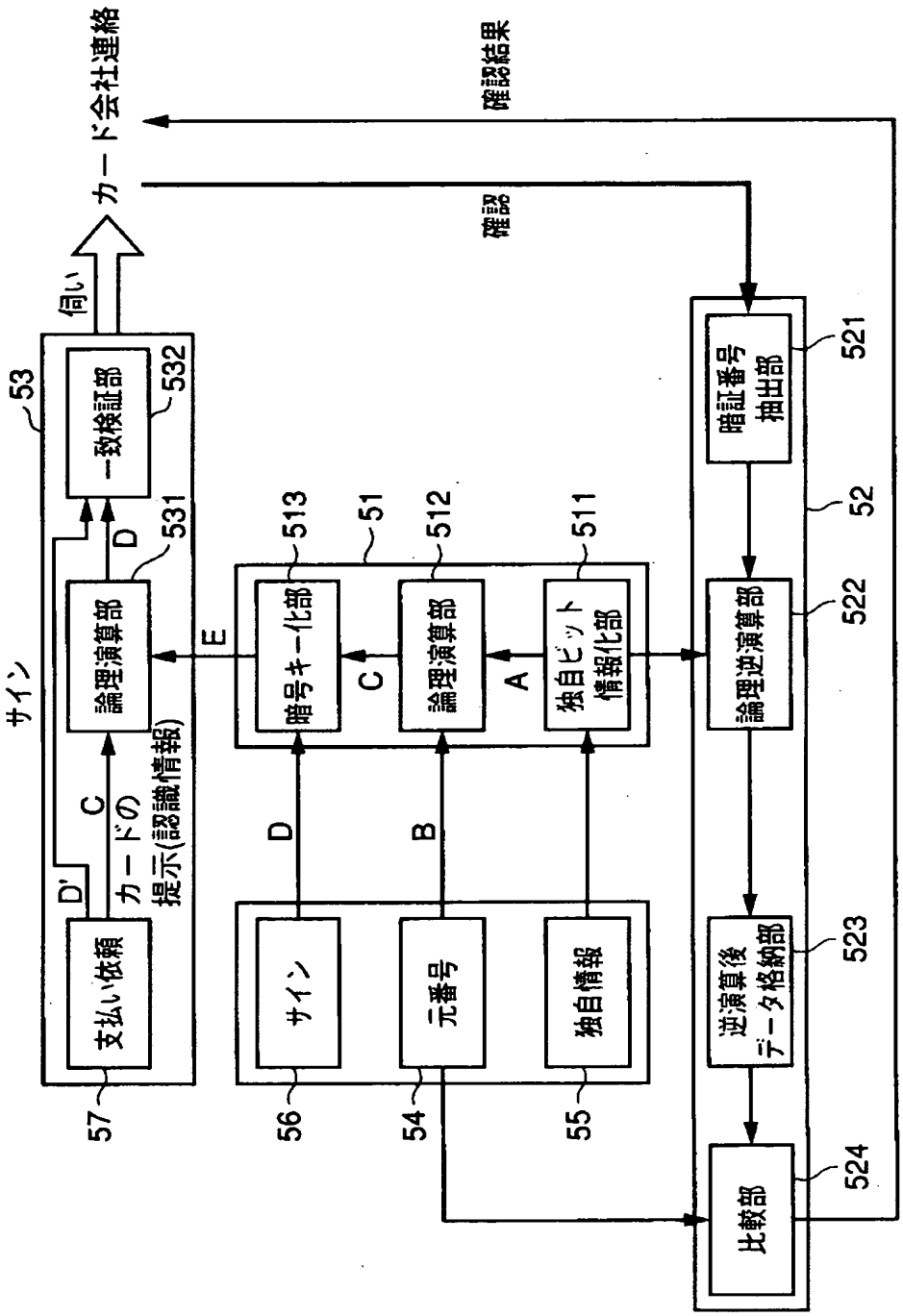
【図３】


カード会社連絡
確認結果
確認
伺い
31
暗号化サービス
314
313
312
311
認証部
認識情報化部
論理演算部
独自ビット情報化部
32
321
322
323
324
認識情報抽出部
論理逆演算部
逆演算後データ格納部
比較部
支払い現場
支払い依頼
35
本人保管
暗証番号
独自情報
33
34

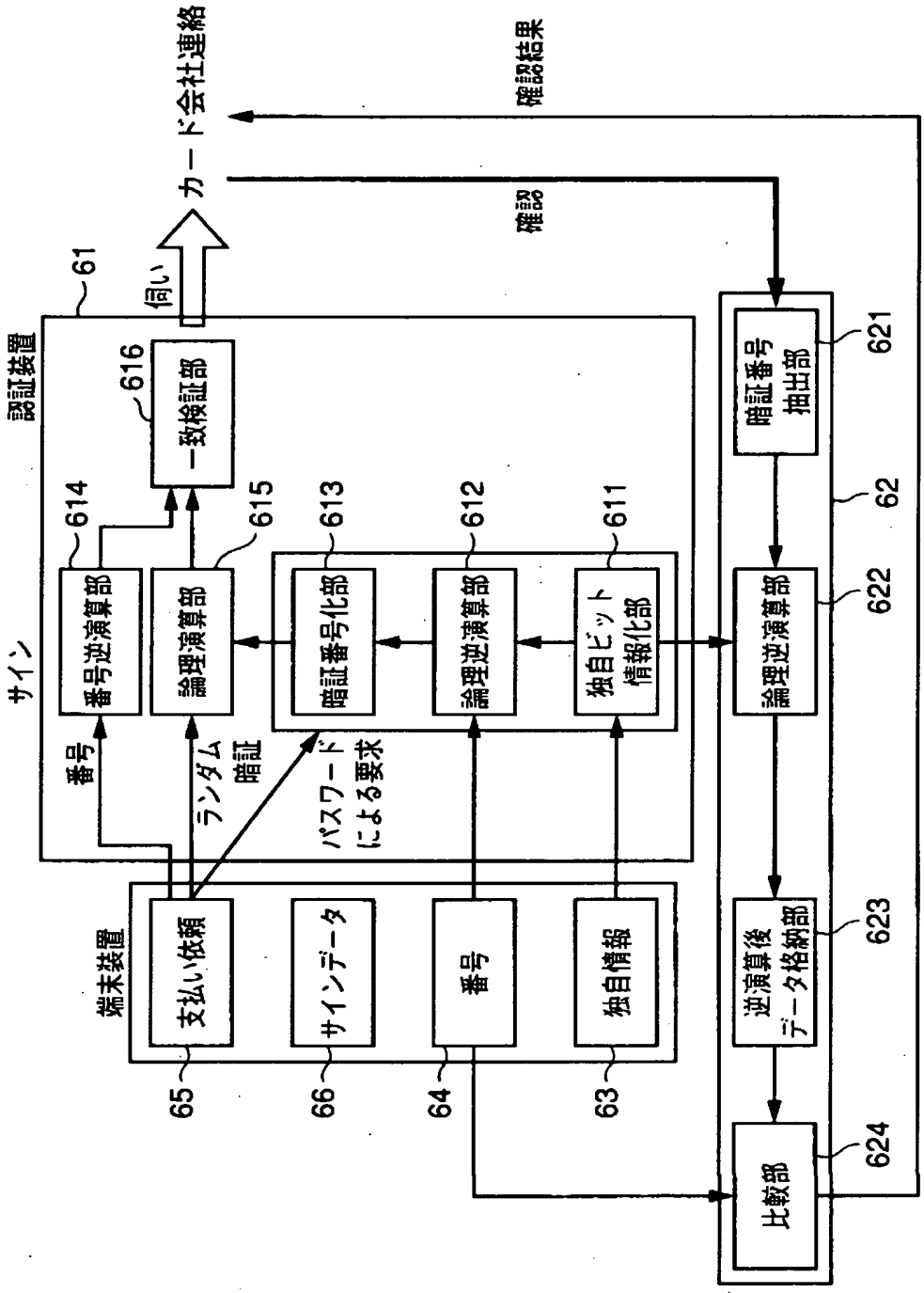
【図４】


カード会社連絡
確認結果
無線連絡
伺い
認証
46
413
41
412
411
421
42
422
423
424
認識情報
認識情報化部
論理演算部
独自ビット情報化部
認識情報抽出部
論理逆演算部
逆演算後データ格納部
比較部
支払い現場
支払い依頼
45
本人保管
暗証番号
43
独自情報
44

【図５】


カード会社連絡
確認結果
確認
伺い
53
一致検証部
532
論理演算部
531
D
サイン
E
暗号キー化部
513
51
論理演算部
512
C
独自ビット情報化部
511
A
暗証番号抽出部
521
52
論理逆演算部
522
D'
C
カードの提示(認識情報)
支払い依頼
57
D
サイン
56
B
元番号
54
独自情報
55
逆演算後データ格納部
523
比較部
524

【図６】


カード会社連絡
確認結果
確認
問い
61
認証装置
サイン
616
一致検証部
614
615
613
612
611
番号逆演算部
論理演算部
暗証番号化部
論理逆演算部
独自ビット情報化部
番号
ランダム暗証
パスワードによる要求
端末装置
支払い依頼
サインデータ
番号
独自情報
65
66
64
63
暗証番号抽出部
621
62
論理逆演算部
622
逆演算後データ格納部
623
比較部
624

【書類名】　　要約書

【要約】

【課題】　電子署名が偽造されて悪用されるのを防止することが可能な認証装置を提供すること。

【解決手段】　論理演算部２１２は、元サイン２３に対して、本人の身体に関連した情報を数値化して得られた独自情報を用いて演算を行なって、暗号化された電子署名を生成する。そして、電子署名付加部２１４は、電子書類２５に電子署名を付加して配布する。したがって、本人の特定が困難となり、電子署名が偽造されて悪用されることを防止することが可能となる。その結果、市場における個人のプライバシおよびプロパティを守ることが可能となる。

【選択図】　　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００６０１３〕

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　東京都千代田区丸の内２丁目２番３号
氏　名　三菱電機株式会社